PCT/JP2004/019488
20.12.2004

日本国特許庁
JAPAN PATENT OFFICE

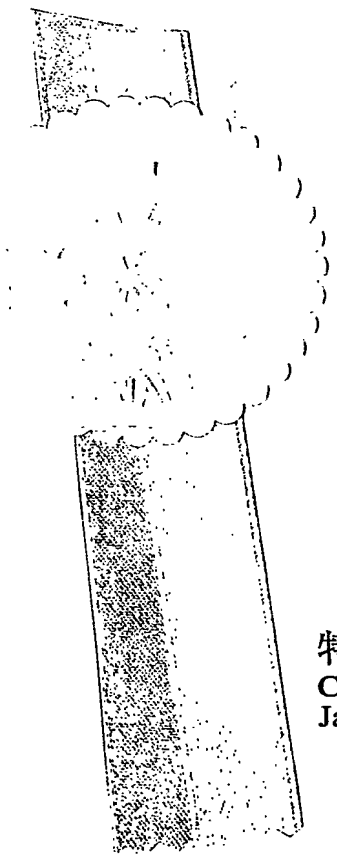
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月１６日

出願番号
Application Number: 特願２００４－００９８６１
[ST. 10/C]: [ＪＰ２００４－００９８６１]

出願人
Applicant(s): 松下電器産業株式会社



２００５年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００４０３５

【書類名】　特許願
【整理番号】　2048150057
【あて先】　特許庁長官殿
【国際特許分類】　G06F
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大原　俊次
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　片山　崇
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置であって、
前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを受信する端末情報受信手段と、
前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、
複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索手段と、
前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段と
を備えることを特徴とする認証用サーバ装置。
【請求項２】
前記認証用サーバ装置は、さらに、
当該認証用サーバ装置の操作者から端末ＩＤを受け付ける受付手段と、
前記受け付けた端末ＩＤが、前記端末情報検索手段に保持されている端末情報に登録されているか否かを判別する未登録判別手段とを備え、
前記端末情報検索手段は、さらに、
前記未登録判別手段において登録されていないと判別された場合のみ、新たに前記所定の端末情報を追加登録する
ことを特徴とする請求項１記載の認証用サーバ装置。
【請求項３】
前記デジタルコンテンツについてのアクセス回数は１回に制限されている場合であって、
前記認証用サーバ装置は、さらに、
前記端末鍵および前記端末ＩＤの組によって特定される端末装置毎に、前記アクセスを受け付けたデジタルコンテンツの履歴を表す情報を蓄積する履歴蓄積手段を備え、
前記不正端末判定手段は、さらに、
同一の前記端末鍵および前記端末ＩＤに係る端末装置から、デジタルコンテンツに対して複数回数アクセスを受け付けた場合は、当該端末装置は不正端末であると判定する
ことを特徴とする請求項１又は２記載の認証用サーバ装置。
【請求項４】
前記端末鍵は、秘密鍵暗号方式における秘密鍵又は公開鍵暗号方式における公開鍵証明書である
ことを特徴とする請求項３記載の認証用サーバ装置。
【請求項５】
ネットワークを介してアクセスしてきた端末装置の中から不正な端末装置を検出する認証用サーバ装置と、ネットワークを介して前記認証用サーバ装置にアクセスし得る端末装置を含む不正端末検出システムであって、
前記端末装置は、
当該端末装置に予め与えられている端末鍵によって生成された検証用データと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを前記認証サーバ装置に送信する端末情報送信手段を備え、
前記認証用サーバ装置は、
前記端末装置から、前記端末鍵に基づいて生成された検証用のデータと前記端末ＩＤとを受信する端末情報受信手段と、
前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段

と、
　複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索手段と、
　前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段と
　を備えることを特徴とする不正端末検出システム。
【請求項６】
　ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する不正端末検出方法であって、
　前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを受信する端末情報受信ステップと、
　前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証ステップと、
　複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索ステップと、
　前記端末鍵検証ステップによって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定ステップと
　を含むことを特徴とする不正端末検出方法。
【請求項７】
　前記不正端末検出方法は、さらに、
　操作者から端末ＩＤを受け付ける受付ステップと、
　前記受け付けた端末ＩＤが、前記端末情報検索ステップに保持されている端末情報に登録されているか否かを判別する未登録判別ステップとを含み、
　前記端末情報検索ステップは、さらに、
　前記未登録判別ステップにおいて登録されていないと判別された場合のみ、新たに前記所定の端末情報を追加登録する
　ことを特徴とする請求項６記載の不正端末検出方法。
【請求項８】
　ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置のためのプログラムであって、
　前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを受信する端末情報受信ステップと、
　前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証ステップと、
　複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索ステップと、
　前記端末鍵検証ステップによって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定ステップと
　をコンピュータに実行させることを特徴とするプログラム。
【請求項９】
　前記プログラムは、さらに、
　操作者から端末ＩＤを受け付ける受付ステップと、
　前記受け付けた端末ＩＤが、前記端末情報検索ステップに保持されている端末情報に登録されているか否かを判別する未登録判別ステップとを含み、

前記端末情報検索ステップは、さらに、
前記未登録判別ステップにおいて登録されていないと判別された場合のみ、新たに前記所定の端末情報を追加登録する
ことを特徴とする請求項８記載のプログラム。

【書類名】明細書
【発明の名称】認証用サーバ装置、不正端末検出方法および不正端末検出システム
【技術分野】
【０００１】
本発明は、不正に製造された端末を検出する装置、方法およびそのシステムに関し、特に、不正に復号鍵が生成されたネットワーク上のＤＶＤプレーヤなどを検出する装置等に関する。
【背景技術】
【０００２】
近年、パッケージコンテンツ（例えば、映像、音声ソフトなど）を格納した種々の記録媒体（例えば、ＤＶＤ(Digital Versatile Disc)など）およびこれらを再生する装置（例えば、ＤＶＤプレーヤなど）が普及すると共に、これらの著作権を保護するため、各種の方策が講じられている。
例えば、ＤＶＤプレーヤに格納されている端末鍵（「デバイス鍵」ともいう。）を用いて、ＤＶＤに記録されている暗号化されたコンテンツを復号する方法がある（従来例１）。この場合、端末鍵は、プレーヤ毎に異なっているものとする。また、ライセンス料の支払いと引き換えに、ライセンサからＤＶＤプレーヤの製造会社に上記ライセンス料に応じた個数の端末鍵が提供される。
【０００３】
一方、通信網に接続されているセンタと複数の端末から構成されるグループ鍵を利用する通信システムにおいて、不正に複製された端末を自動的に発見して排除する方法も提案されている（例えば、特許文献１参照）。これは、通信網に接続されているセンタが、端末に新規のグループ鍵を配布する際に、端末から端末ＩＤと端末乱数をセンタの公開鍵で暗号化した情報とを受信し、通信ログを検索して、同一端末ＩＤで端末乱数の異なる端末の有無を検査する。該当する端末があれば、複製端末であると判断して、グループ鍵を配布しない。この場合、各端末で発生させる乱数は複製が困難であり、複製された端末は同じ乱数を生成できないので、複製端末の存在を検出することができる。
【特許文献１】特開２００２－２１７８９０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、上記従来例１の方法では、ライセンス料で規定された個数を越えた数の端末鍵を生成したり、不正な解析によって正当なＤＶＤプレーヤから端末鍵を解読し、解読した端末鍵を埋め込んだＤＶＤプレーヤを不正に複製する場合も生じ得る。その場合、「複数の端末に同一の端末鍵が格納されていること」や「不正なＤＶＤプレーヤに格納されている端末鍵がどの正当なＤＶＤプレーヤの端末鍵なのか」を検出することは困難であるという問題がある。
【０００５】
図１０は、上記従来例１における問題の概要を説明するための図である。図１０に示されるように、機器製造メーカ１００は、ライセンサ１５０に１万台分のライセンス料を支払って正当に１万個の端末鍵（KA1～KA10000）をライセンサ１５０（又はライセンサ１５０から委託された鍵管理会社）から受け取って各端末に格納している。
しかし、機器製造メーカ２００のように、ライセンサ１５０に１台分のライセンス料を支払っただけで、１個の端末鍵（KB1）を不正に９９９９個コピーして１万台の端末に格納することも可能である。さらに、機器製造メーカ３００のように、ライセンサ１５０にライセンス料を支払うことなく、機器製造メーカ２００が製造した端末２０１を入手し、その端末に格納されている端末鍵KB1を不正に複製して同一の端末鍵KB1を全端末に格納することも可能である。
【０００６】
また、上記特許文献１の方法は、不正に複製された端末か否かを検出することは可能で

あるが、「不正なＤＶＤプレーヤに格納されている端末鍵がどの正当なＤＶＤプレーヤの端末鍵なのか」を検出することは困難である。

そこで、本発明は、複数の端末に同一の端末鍵が格納されていることや不正端末にどの正当な端末の端末鍵が格納されているかを検出し得る認証用サーバ装置、不正端末検出方法などを提供することを目的とする。

【課題を解決するための手段】

【０００７】

上記の目的を達成するために、本発明に係る認証用サーバ装置は、ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置であって、前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを受信する端末情報受信手段と、前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索手段と、前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段とを備える。

【０００８】

これにより、たとえ端末鍵が不正に生成されたり複製されたりした場合であっても、端末鍵に対応づけて登録されている各端末に付加された端末ＩＤが異なる場合は、不正な端末か否かを容易に判定することができる。

さらに、上記目的を達成するために、本発明に係る不正端末検出システムは、ネットワークを介してアクセスしてきた端末装置の中から不正な端末装置を検出する認証用サーバ装置と、ネットワークを介して前記認証用サーバ装置にアクセスし得る端末装置を含む不正端末検出システムであって、前記端末装置は、当該端末装置に予め与えられている端末鍵によって生成された検証用データと、端末装置毎にその製造後に付加された識別情報である端末ＩＤとを前記認証サーバ装置に送信する端末情報送信手段を備え、前記認証用サーバ装置は、前記端末装置から、前記端末鍵に基づいて生成された検証用のデータと前記端末ＩＤとを受信する端末情報受信手段と、前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、複数の端末装置について、前記端末ＩＤを含む所定の端末情報を予め保持し、前記受信した端末ＩＤについて検索を試みる端末情報検索手段と、前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末ＩＤと異なる端末ＩＤが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段とを備える。

【０００９】

これにより、たとえ端末鍵が不正に生成されたり複製されたりした場合であっても、端末鍵に対応づけて登録されている各端末に付加された端末ＩＤが異なる場合は、認証用サーバ装置にアクセスしてきた端末装置が不正な端末か否かを容易に判定することができるので、ネットワークを介して配信されるデジタルコンテンツに対する著作権侵害を最小限に抑えることが可能となる。

【００１０】

なお、本発明は、上記認証用サーバ装置が備える特徴的な手段をステップとする不正端末検出方法として実現したり、それらステップをパーソナルコンピュータ等に実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをＤＶＤ等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは云うまでもない。

【発明の効果】

【００１１】

以上の説明から明らかなように、本発明によれば、不正な端末を容易に検出し、ネットワークを介して配信されるデジタルコンテンツに対する著作権侵害を最小限に抑えること

が可能となる。
以上のように、本発明により、端末鍵と端末ＩＤとを組み合わせて検証に用いることによって不正に製造された端末装置の検出をより容易に行うことが可能となり、パッケージコンテンツの著作権を適正に保護することができる。従って、インターネット等のネットワークを介してＤＶＤ等に格納されているデジタル著作物の配信や流通が活発になってきた今日において、本願発明の実用的価値は極めて高い。
【発明を実施するための最良の形態】
【００１２】
以下、本発明に係る実施の形態について、図面を参照しながら詳細に説明する。
図１は、本実施の形態に係る不正端末検出システム５の概要を示すブロック図である。図１の不正端末検出システム５は、ネットワーク３０を利用して不正に製造された端末（例えば、ＤＶＤプレーヤなど）を検出するためのシステムであり、上記端末の検出を行うセンタ５０の認証サーバ４０と検査対象のＤＶＤ端末２０（少なくとも１台存在している。）とが、例えば、インターネットなどのネットワーク３０を介して接続されている。ここで、「不正に製造」とは、正当な権限を有さずに製造することをいい、例えば、暗号化されているコンテンツ（例えば、ＤＶＤ－ＲＯＭに格納されている暗号化されたパッケージソフト）を復号するために必要な端末鍵を、不正な方法で上記パッケージコンテンツを再生するための端末（例えば、ＤＶＤプレーヤ）に格納する場合が該当する。
【００１３】
ここで、本システム５における不正端末の検出方法の概要について説明する。本実施の形態では、ＤＶＤ－ＲＯＭパッケージ１０のユーザの利用形態として、以下の３つの場合を想定する。
(１)ＤＶＤ－ＲＯＭパッケージ１０に格納されているコンテンツ（例えば、映画のコンテンツ）そのものを利用する。
(２)上記(１)のコンテンツに関連するサブコンテンツ（例えば、映画のコンテンツに対応する無料の字幕用のデータコンテンツ）をネットワーク３０上のセンタ５０から入手して利用する。
(３)上記(１)のコンテンツに関連する暗号化されたサブコンテンツ（例えば、ディレクターズカット映像やおまけ映像など）を、さらに料金を支払ってネットワーク３０上のセンタ５０から入手して利用する。この場合は、料金を支払うことによって、上記サブコンテンツを復号するための鍵（復号鍵）をセンタ５０から入手することとする。
【００１４】
そこで、上記(２)および(３)の場合は、ユーザは、ＤＶＤ端末２０を介して必ずセンタ５０に接続するため、その際に認証サーバ４０を用いて自動的に当該ＤＶＤ端末２０を認証することとする。具体的には、ＤＶＤ端末２０から認証サーバ４０にサブコンテンツの送信を要求する際に、いわゆる「チャレンジ－レスポンス型認証方式」を用いてＤＶＤ端末２０を認証する。
【００１５】
例えば、秘密鍵暗号方式を用いて「チャレンジ－レスポンス型認証」を行う場合は、認証側（本実施の形態では認証サーバ４０）と被認証側（本実施の形態ではＤＶＤ端末２０）が同一の端末鍵（秘密鍵）を保持する。そして、ＤＶＤ端末２０は、認証サーバ４０に認証要求を送信する。ＤＶＤ端末２０から認証要求を受信した認証サーバ４０は、乱数を生成してＤＶＤ端末２０に送信する。ＤＶＤ端末２０は、自身が保持する端末鍵で受信した乱数の暗号化を行い、端末ＩＤと共に認証サーバ４０に送信する。ＤＶＤ端末２０から、乱数を暗号化したデータと端末ＩＤとを受信した認証サーバ４０は、予め保持している、ＤＶＤ端末２０が保持するものと同一の端末鍵で乱数を復号して、ＤＶＤ装置２０が保持する端末鍵が正当な端末鍵か否かを検証する。さらに、認証サーバ４０は、ＤＶＤ端末２０から受信した端末ＩＤが、予め登録している端末ＩＤと一致するか否かを調べる。もし、認証サーバ４０からＤＶＤ端末２０に送信した乱数と認証サーバ４０が復号した乱数とが一致しない場合（又は乱数を復号できない場合）、認証サーバ４０は、そのＤＶＤ端

末２０は「不正な端末である」と判定する。特に、乱数は正しく復号できたが、端末ＩＤが一致しない場合は、ＤＶＤ装置２０の端末鍵は「不正に複製された」と判断する。

【００１６】

一方、公開鍵暗号方式を用いて「チャレンジーレスポンス型認証」を行う場合の一例を以下に示す。認証サーバ４０は、証明書発行局の公開鍵を保持している。ＤＶＤ端末２０は、認証サーバ４０に、認証要求と共に自身の公開鍵証明書を送信する。認証サーバ４０は、保持している証明書発行局の公開鍵を用いてＤＶＤ端末２０から受信した公開鍵証明書の正当性を検証する。公開鍵証明書が正当なものであると確認した場合、認証サーバ４０は、乱数を生成してＤＶＤ端末２０に送信する。ＤＶＤ端末２０は、自身が保持する端末鍵（秘密鍵）を用いて受信した乱数にデジタル書名を施し、端末ＩＤと共に認証用データとして認証サーバ４０に送信する。これにより、認証サーバ４０は、検証済みの公開鍵証明書に対応するＤＶＤ端末２０の公開鍵で、受信した認証用データの正当性を検証する。受信した認証用データの正当性が確認できない場合、認証サーバ４０は、ＤＶＤ端末２０は「不正な端末である」と判定し、認証用データの正当性が確認できた場合は、ＤＶＤ端末２０は「正当な端末である」と判定する。

【００１７】

なお、「端末鍵」は、個々のＤＶＤ端末２０によって異なる鍵であり、上記のように秘密鍵暗号方式における秘密鍵（この場合、認証サーバ４０とＤＶＤ端末２０とは、同一の秘密鍵を保有する。）や、公開鍵暗号方式における秘密鍵（この場合、ＤＶＤ端末２０は、認証サーバ４０に自身の公開鍵証明書を送信し、認証サーバ４０は、受信した公開鍵証明書に含まれているＤＶＤ端末２０の公開鍵を保持する。）などがある。ここで、「公開鍵証明書」には、ＤＶＤ端末の「形式＋連番」、「端末ＩＤ」、「公開鍵」、および「端末ＩＤと公開鍵とを連結したデータに対するデジタル署名」等が含まれることとする。また、「端末ＩＤ」とは、ＤＶＤ端末を識別し得る情報をいい、例えば、ユーザが上記ＤＶＤ端末２０の購入時又はサービスの加入時に登録する際に特定されるユーザＩＤやサービスＩＤが該当する。端末ＩＤのその他の例としては、ＩＰアドレスやＭＡＣアドレス、ユーザ本人が記入する名前やユーザが任意につけるニックネームなどがある。なお、端末ＩＤは、上記購入時又はサービスの加入時に、既に登録されている他の端末ＩＤと重複していないことを確認して登録することとしてもよい。

【００１８】

図２は、本システム５におけるＤＶＤ端末２０と認証サーバ４０の機能構成を示したブロック図である。図２のＤＶＤ端末２０は、ＤＶＤ－ＲＯＭパッケージ１０に格納されているコンテンツの復号及び再生を行う機能を有すると共に、ネットワーク３０を介して認証サーバ４０から各種のサブコンテンツを入手する機能を有するＤＶＤプレーヤであり、通信制御部２１、全体制御部２２、復号再生部２３、入出力部２４及び端末情報記憶部２５を備える。なお、ＤＶＤ端末２０における各構成要素は、バス２９を介して相互に接続されている。

【００１９】

通信制御部２１は、ネットワーク３０を介して認証サーバ４０と通信を行うための制御を行う。全体制御部２２は、例えば、ＲＡＭやＲＯＭ等を備えるマイクロコンピュータであり、ＤＶＤ端末２０の全体を制御する。復号再生部２３は、ＤＶＤ－ＲＯＭパッケージ１０に格納されている、暗号化されているコンテンツの復号および再生を行う。入出力部２４は、スイッチ類や液晶パネル等を備え、ユーザからの操作を受け付けると共に、必要な情報をユーザに提示する。端末情報記憶部２５は、例えば、セキュアな（対タンパ性を有する）ＲＡＭであり、端末鍵（各種の秘密鍵）、公開鍵、公開鍵証明書等や端末ＩＤを記憶する。ここで、許可されていない第３者は、端末情報記憶部２５に記憶されている情報を参照したり、更新したりすることができないこととする。

【００２０】

一方、図２の認証サーバ４０は、ネットワーク３０を介してサブコンテンツの入手を要求してきた端末の認証を行うサーバであり、通信制御部４１、全体制御部４２、端末認証

部４３、入出力部４４および認証用ＤＢ４５を備える。なお、認証サーバ４０における各構成要素は、バス４９を介して相互に接続されている。

通信制御部４１は、上記ＤＶＤ端末２０における通信制御部２１と同様、認証サーバ４０の通信機能の制御を行う。全体制御部４２は、例えば、ＲＡＭやＲＯＭ等を備えるマイクロコンピュータであり、認証サーバ４０の全体を制御する。端末認証部４３は、認証用ＤＢ４５に格納されている端末鍵や端末ＩＤ、ＤＶＤ端末から受信した端末ＩＤ等に基づいて、当該ＤＶＤ装置を認証する。

【００２１】

入出力部４４は、キーボードや液晶パネル等を備え、センタ５０の管理者等からの操作を受け付けると共に、必要な情報を管理者等に提示する。認証用ＤＢ４５は、ＤＶＤ端末毎に端末鍵（各種の秘密鍵）、公開鍵、公開鍵証明書等および端末ＩＤを関連づけて登録し、又は記憶している。

図３は、上記認証用ＤＢ４５に記憶されているデータの一例を示す。図３（ａ）は、認証用ＤＢ４５に記憶されている、ＤＶＤ端末の形式＋連番、端末ＩＤ、端末鍵および各ＤＶＤ端末が行ったサブコンテンツの送信要求履歴を対応付けて格納するためのテーブル例である。この「形式＋連番」により、ＤＶＤ端末を識別することができる。なお、図３（ａ）の形式＋連番、端末鍵は、ＤＶＤ端末が製造された時点で確定するデータであり、端末ＩＤは、上述したように、購入時又はサービスの加入時に確定（製造後に認証サーバ４０に登録）するものとする。

【００２２】

また、図３（ｂ）は、上記認証用ＤＢ４５に憶されている、ＤＶＤ端末の形式、端末鍵の総数およびアクセス数を対応付けて格納するためのテーブル例である。

【００２３】

次に、以上のように構成される不正端末検出システム５の動作について説明する。図４は、上記の利用形態(２)、即ち、ＤＶＤ端末２０が無料のサブコンテンツを入手する場合のＤＶＤ端末２０－認証サーバ４０間における通信シーケンス図である。

【００２４】

最初に、ＤＶＤ端末２０は、認証サーバ４０にサブコンテンツの送信要求を行う（Ｓ３０２）。これにより、認証サーバ４０は、乱数Ｒを生成し（Ｓ３０４）、ＤＶＤ端末２０に送信する（Ｓ３０６）。すると、ＤＶＤ端末２０は、端末情報記憶部２５に記憶している端末鍵と端末ＩＤを読み出し、端末鍵（ＳＫ＿Ｘ）で、受信した乱数Ｒを暗号化（＝Ｒｅｓ）し（Ｓ３０８）、このＲｅｓと端末ＩＤ（ＩＤ＿Ｘ）とを認証サーバ４０に送信する（Ｓ３１０）。

【００２５】

次に、認証サーバ４０は、ＤＶＤ端末２０から受信した暗号化された乱数Ｒ及び端末ＩＤについて検証し、ＤＶＤ端末２０が正当な端末か否かを認証する（Ｓ３１２：認証処理１）。ＤＶＤ端末２０が正当な端末であると判定した場合、認証サーバ４０は、ＤＶＤ端末２０に対して要求通りのサブコンテンツを送信する（Ｓ３１４）。もし、ＤＶＤ端末２０が不当な端末であると判定した場合、認証サーバ４０は、ＤＶＤ端末２０に対して、エラーに応じて特定したエラーメッセージを送信する（Ｓ３１４括弧書き）。

【００２６】

一方、ＤＶＤ端末２０は、認証サーバ４０からサブコンテンツを受信した場合は、これを記録又は再生し（Ｓ３１６）、エラーメッセージを受信した場合は、入出力部２４にエラーメッセージを表示する（Ｓ３１６）。

エラーメッセージとしては、例えば、「この端末では、本サービスを受けることができません。」、「この端末は、いずれＲＯＭパッケージの再生もできなくなります。」というメッセージ又は警告等を現地語（例えば、ＤＶＤ端末が販売される地域の言語など）で表示する。

【００２７】

なお、エラーメッセージとしての表示ではないが、コンテンツによっては、定期的に更

新される無料の「おまけコンテンツ」を提供するというサービスもあり、この場合は、定期的に端末がセンタに自動でアクセスを行うため、入出力部２４に、「おまけコンテンツの自動更新を行うため、ネットワークを接続した状態にしておいて下さい。」等の表示を行い、上記認証の実施を確保することとしてもよい。

【００２８】

また、図５は、上記の利用形態(3)、即ち、ＤＶＤ端末２０が有料のサブコンテンツを入手する場合のＤＶＤ端末２０－認証サーバ４０間における通信シーケンス図である。なお、図５においては、認証処理１（Ｓ３１２）までは、上記図４と同じ処理であるため、説明を省略する。

認証サーバ４０は、ＤＶＤ端末２０から要求されたサブコンテンツが有料か否かを判別し、有料の場合は、ＤＶＤ端末２０に対して料金の支払い要求を行う（Ｓ３２２）。「料金の支払い要求」を受信したＤＶＤ端末２０は、料金支払処理を実行し（Ｓ３２４）、認証サーバ４０に料金支払済み通知を行う（Ｓ３２６）。

【００２９】

ＤＶＤ端末２０から「料金支払済み通知」を受信した認証サーバ４０は、ＤＶＤ端末２０にサブコンテンツ（又はエラーメッセージ）を送信する（Ｓ３１４）。なお、以下の処理は、図４におけるＳ３１２の処理と同じであるため、図５においては省略している。

図６は、上記図４及び図５に示した、認証サーバ４０における認証処理１（Ｓ３１２）の処理内容を示すフローチャートである。

【００３０】

最初に、端末認証部４３は、通信制御部４１を介してＤＶＤ端末２０から端末ＩＤ（ＩＤ＿Ｘ）と暗号化された乱数Ｒ（＝Ｒｅｓ）とを受信すると、認証用ＤＢ４５に保持している、ＤＶＤ端末２０と同一の端末鍵（ＩＤ＿Ｘ）で暗号化された乱数Ｒを復号する（Ｓ４０２）。

復号した結果、乱数Ｒが正しくない（又は復号できない）場合（Ｓ４０４：Ｎｏ）、端末認証部４３は、ＤＶＤ端末２０が正しい端末鍵を有さないＤＶＤ端末であると判定し、その旨のエラーメッセージ等を特定し、警告通知を行なうことを決定する（Ｓ４１０）。

【００３１】

一方、復号した結果、乱数Ｒが正しい場合（Ｓ４０４：Ｙｅｓ）、端末認証部４３は、さらに、乱数Ｒの復号に用いた端末鍵とＤＶＤ端末２０から受信した端末ＩＤ（ＩＤ＿Ｘ）との組について認証用ＤＢ４５を検索する（Ｓ４０６）。そして検索した結果、上記端末鍵に対応する端末ＩＤ（ＩＤ＿Ｘ）がある場合（Ｓ４０８：Ｎｏ）、端末認証部４３は、上記端末ＩＤおよび暗号化された乱数Ｒを送信してきた端末は「正当な端末」であると判定してネットワークの接続を許可すること（以下、「ネット接続許可」という。）を決定する。

【００３２】

しかし、受信した端末ＩＤが上記端末鍵に対応する端末ＩＤでない場合（Ｓ４０８：Ｙｅｓ）、端末認証部４３は、「複数のＤＶＤ端末に同一の端末鍵が格納されている」と判定してエラーメッセージ等を特定し、上記ＤＶＤ端末２０に警告通知を行なうことを決定する（Ｓ４１４）。

以上のように、本実施の形態に係る認証サーバによれば、上記の端末鍵と端末ＩＤとを組み合わせて端末の認証に使用することにより、より確実に不正な端末か否かを判別することが可能となる。

【００３３】

（変形例１）

上記実施の形態においては、認証サーバ４０が、ＤＶＤ端末２０から受信した暗号化された乱数Ｒおよび端末ＩＤに基づいて、当該ＤＶＤ端末２０が正当か否かを判定する実施例について説明したが、異なるＤＶＤ端末が、同一の端末鍵および同一の端末ＩＤを有している場合は、それらのＤＶＤ端末が正当か否かを判別することは困難である。そこで、本変形例では、無料のサブコンテンツを受信できる回数が１回に限定されており、同一の

端末鍵および同一の端末ＩＤを有するＤＶＤ端末から複数回アクセスがあった場合は、当該端末は「複製された端末鍵を有する不正な端末」あると判定する。例えば、端末鍵の総数が１０，０００であるのに、１８，５００回のアクセスがあった場合が該当する（上記図３（ｂ）参照）。

【００３４】

図７は、本変形例における、上記図４又は図５の認証処理（Ｓ３１２）の処理内容を示すフローチャートである。上記図４又は図５のフローチャートと異なる点は、認証用ＤＢ４５を参照して過去に同一のサブコンテンツの送信要求があった場合は（Ｓ５０２：Ｙｅｓ）、当該ＤＶＤ端末は「複製された端末鍵を有する不正な端末」であると判定する点である。

【００３５】

以上のように、本変形例における認証サーバによれば、たとえ、同一の端末鍵および同一の端末ＩＤを有するＤＶＤ端末が複数ある場合は、アクセス回数を計数することによって不正な端末か否かを判別することが可能となる。

【００３６】

（変形例２）

上記の実施の形態においては、予め認証サーバとＤＶＤ端末が共有する秘密鍵（共通鍵）を用いて、認証サーバがＤＶＤ端末から受信した暗号化された乱数Ｒおよび端末ＩＤに基づいて、当該ＤＶＤ端末が正当な装置か否かを判定する実施例について説明したが、本変形例では、公開鍵暗号方式を用いて不正な端末を検出する実施例について説明する。本変形例の場合、端末ＩＤと端末鍵との組は、認証サーバとの認証後に登録することとしてもよいこととする。

【００３７】

なお、本変形例における認証サーバ及びＤＶＤ端末の機能構成は、公開鍵暗号システム及びデジタル署名を用いる以外は、上記実施の形態における認証サーバ４０及びＤＶＤ端末２０と同じである。

【００３８】

図８は、本変形例の認証サーバ４０－ＤＶＤ装置２０間における通信シーケンス図である。

最初に、ＤＶＤ端末２０は、認証サーバ４０にサブコンテンツの送信要求を行う（Ｓ３０２）。これにより、認証サーバ４０は、Ｃｅｒｔ＿Ｘを送信するようにＤＶＤ端末２０に要求する（Ｓ８０２）。ここで、「Ｃｅｒｔ＿Ｘ」とは、端末ＩＤ、端末鍵（ＳＫ＿Ｘ）に対応する公開鍵（ＰＫ＿Ｘ）と上記端末ＩＤと公開鍵とを連結したデータに対する認証局ＣＡ（図示せず）のデジタル署名（Ｓｉｇｎ＿Ｘ）を含むデータをいう。

これにより、ＤＶＤ端末２０は、生成したＣｅｒｔ＿Ｘを認証サーバ４０に送信し（Ｓ８０４、Ｓ８０５）する。

【００３９】

次に、ＤＶＤ端末２０からＣｅｒｔ＿Ｘを受信すると、認証サーバ４０は、証明書確認用公開鍵（ＰＫ＿ＣＡ）を用いてＣｅｒｔ＿Ｘ内のデジタル署名Ｓｉｇｎ＿Ｘが、公開鍵（ＰＫ＿Ｘ）と端末ＩＤとを連結したデータに対するデジタル署名であるか否かを検証する（Ｓ８１０）。ここで、Ｓｉｇｎ＿Ｘが正当であると確認できた場合、認証サーバ４０は、乱数Ｒを生成してＤＶＤ端末２０に送信する（Ｓ８１２）。

【００４０】

すると、ＤＶＤ端末２０は、装置内に保有する端末鍵（ＳＫ＿Ｘ）で乱数Ｒに対してデジタル署名を施して（＝Ｓｉｇｎ＿Ｒ）（Ｓ８１４）、認証サーバ４０に送付する（Ｓ８１６）。

この後、認証サーバ４０は、上記のように受信した端末ＩＤ、公開鍵について認証を行なう（Ｓ８１８）。

【００４１】

認証の結果、上記端末ＩＤ及び公開鍵の正当性が確認できた場合は、ＤＶＤ端末２０に

サブコンテンツを送信する（S３１４）。一方上記端末ＩＤ及び公開鍵の正当性が確認できない場合は、ＤＶＤ端末２０にエラーメッセージを送信する（Ｓ８１８括弧書き）。なお、ＤＶＤ端末２０側で、サブコンテンツを受信する（又はエラーメッセージを表示する）処理（Ｓ３１６）は、上記、図４又は図５の場合と同様である。

【００４２】

図９は、上記図８における認証処理２（Ｓ８１８）の流れを示すフローチャートである。

最初に、認証サーバ４０は、端末鍵（ＳＫ＿Ｘ）に対応する公開鍵（ＰＫ＿Ｘ）で上記Ｓｉｇｎ＿Ｒが、乱数Ｒに対する端末鍵（ＳＫ＿Ｘ）によるデジタル署名であるか否かを検証する（Ｓ９０２）。この場合、Ｓｉｇｎ＿Ｒが正当であると確認できない場合は（Ｓ９０３：Ｎｏ）、本認証を中止してその旨をＤＶＤ端末２０に通知する（Ｓ９０４）。

【００４３】

一方、Ｓｉｇｎ＿Ｒが正当であると確認できた場合（Ｓ９０３：Ｙｅｓ）、認証サーバ４０は、ＤＶＤ端末２０の端末ＩＤと公開鍵との組の有無について、認証用ＤＢ４５を検索する（Ｓ９０５）。

ここで、もし、同一の公開鍵がない場合は（Ｓ９０６：Ｎｏ）、新規な正当なＤＶＤ端末であると判断し、上記端末ＩＤ及び公開鍵を認証用ＤＢ４５に登録し、ネット接続の許可を決定する（Ｓ９１４）。

【００４４】

一方、公開鍵については同一のものがあったが、端末ＩＤについては異なっていた場合は（Ｓ９０８：Ｎｏ）、複数のＤＶＤ端末に同一の端末鍵が格納されていると不正な端末であると判断し、その旨の警告を通知することとする（Ｓ９１０）。なお、公開鍵も端末ＩＤも同一のものが存在する場合は、当該ＤＶＤ端末は正当な端末であると判定し、ネット接続の許可を決定する（Ｓ９１４）。

【００４５】

なお、上記実施の形態に係る不正端末検出システム５においては、センタ５０が１ヶ所の場合の実施例について説明したが、センタが複数ある場合であっても、上記端末鍵および端末ＩＤの組の情報を全てのセンタで共有することによって（例えば、端末鍵および端末ＩＤの組の情報を格納する共通のサーバを用意する。）、本発明を適用することが可能である。

【００４６】

さらに、上記の実施の形態及び変形例においては、検証端末としてＤＶＤ端末を例に挙げて説明したが、ＤＶＤ端末に限定するものではなく、ＣＤプレーヤやパーソナルコンピュータ等、デジタルコンテンツに関して各種暗号システムを適用し得る装置であってもよい。

【産業上の利用可能性】

【００４７】

本発明の認証用サーバ装置、不正端末検出方法および不正端末検出システムは、デジタルコンテンツの著作権を保護しながらネットワークを介して暗号化されたコンテンツを配信し得るコンテンツサーバ装置として適用が可能であり、著作権を保護しながらネットワークを介して暗号化されたコンテンツを配信するネットワークシステムとして有用である。

【図面の簡単な説明】

【００４８】

【図１】本実施の形態に係る不正端末検出システムの概要を示すブロック図である。

【図２】不正端末検出システムにおけるＤＶＤ端末と認証サーバの機能構成を示したブロック図である。

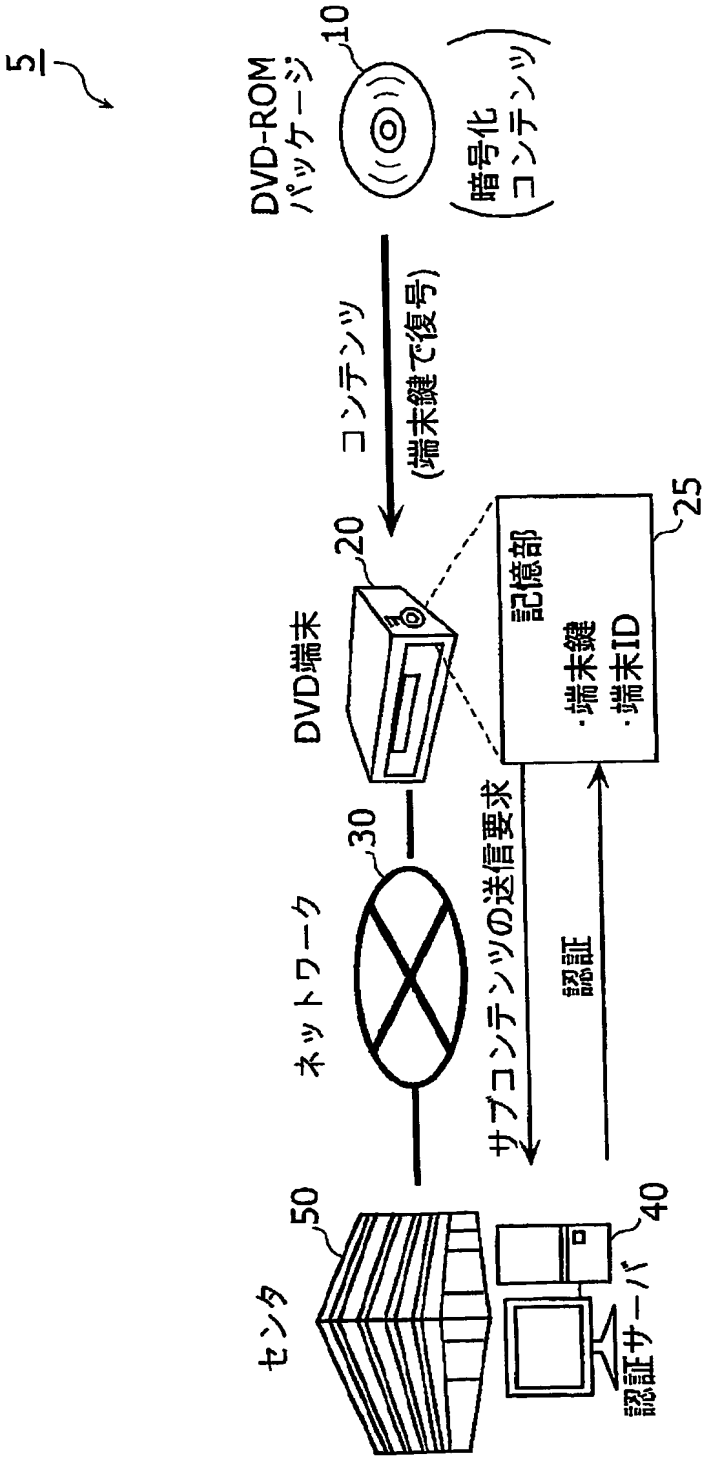
【図３】（ａ）は、認証サーバの認証用ＤＢに記憶されているデータの一例を示す。（ｂ）は、認証サーバの認証用ＤＢに記憶されているデータの一例を示す。

【図４】ＤＶＤ端末が無料のサブコンテンツを入手する場合のＤＶＤ端末－認証サー

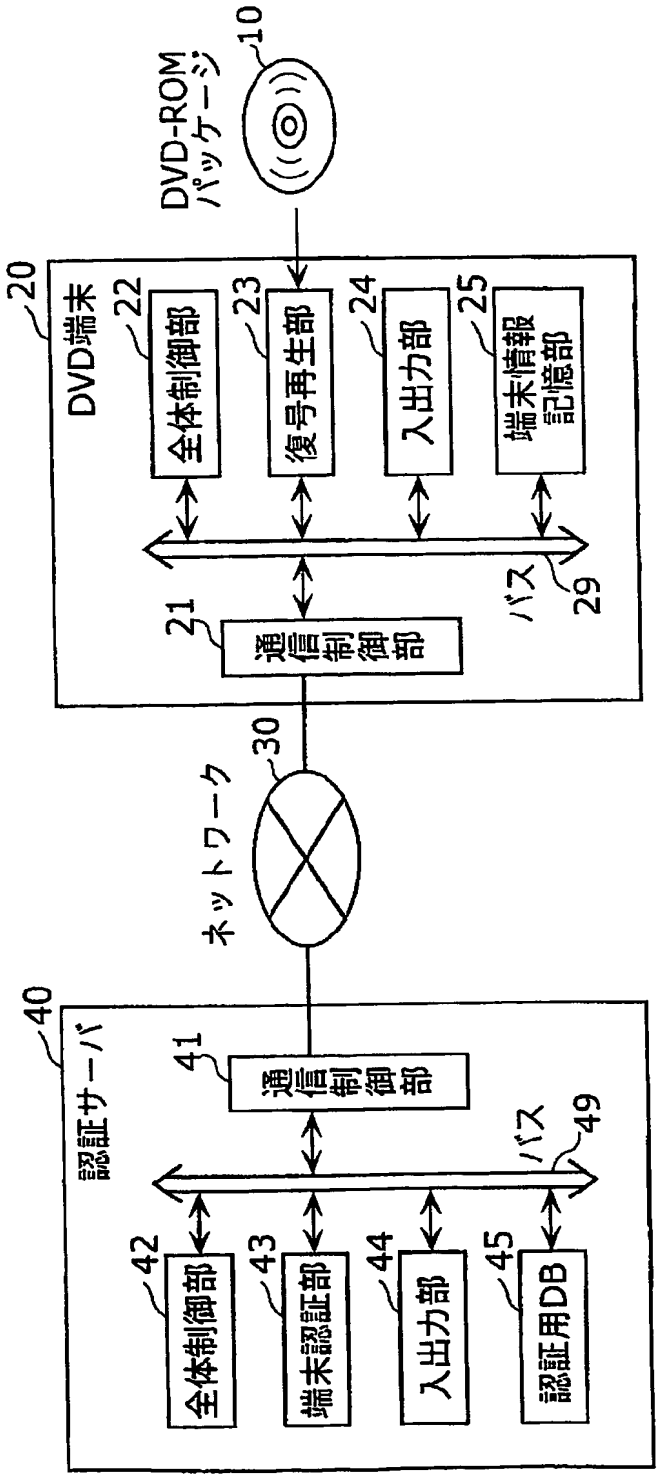
バ間における通信シーケンス図である。
【図５】ＤＶＤ端末が有料のサブコンテンツを入手する場合のＤＶＤ端末－認証サーバ間における通信シーケンス図である。
【図６】図４又は図５に示される、認証サーバにおける認証処理１の流れを示すフローチャートである。
【図７】図４又は図５に示される、認証サーバにおける認証処理１の変形例の流れを示すフローチャートである。
【図８】変形例２におけるＤＶＤ端末－認証サーバ間における通信シーケンス図である。
【図９】図８に示される、認証サーバにおける認証処理２の流れを示すフローチャートである。
【図１０】従来例１における問題の概要を説明するための図である。
【符号の説明】
【００４９】

５	不正端末検出システム
１０	ＤＶＤ－ＲＯＭパッケージ
２０	ＤＶＤ端末
２１	通信制御部
２２	全体制御部
２３	復号再生部
２４	入出力部
２５	端末情報記憶部
３０	ネットワーク
４０	認証サーバ
４１	通信制御部
４２	全体制御部
４３	端末認証部
４４	入出力部
４５	認証用ＤＢ
５０	センタ
１００	機器製造メーカ
１５０	ライセンサ
２００	機器製造メーカ
３００	機器製造メーカ

【書類名】図面
【図１】


5
DVD-ROM
パッケージ
10
暗号化
コンテンツ
コンテンツ
(端末鍵で復号)
20
DVD端末
25
記憶部
・端末鍵
・端末ID
30
ネットワーク
サブコンテンツの送信要求
認証
50
センタ
40
認証サーバ

【図２】


DVD-ROM
パッケージ
10
20
DVD端末
22
全体制御部
23
復号再生部
24
入出力部
25
端末情報
記憶部
バス
29
21
通信制御部
30
ネットワーク
40
認証サーバ
41
通信制御部
バス
49
42
全体制御部
43
端末認証部
44
入出力部
45
認証用DB

【図３】

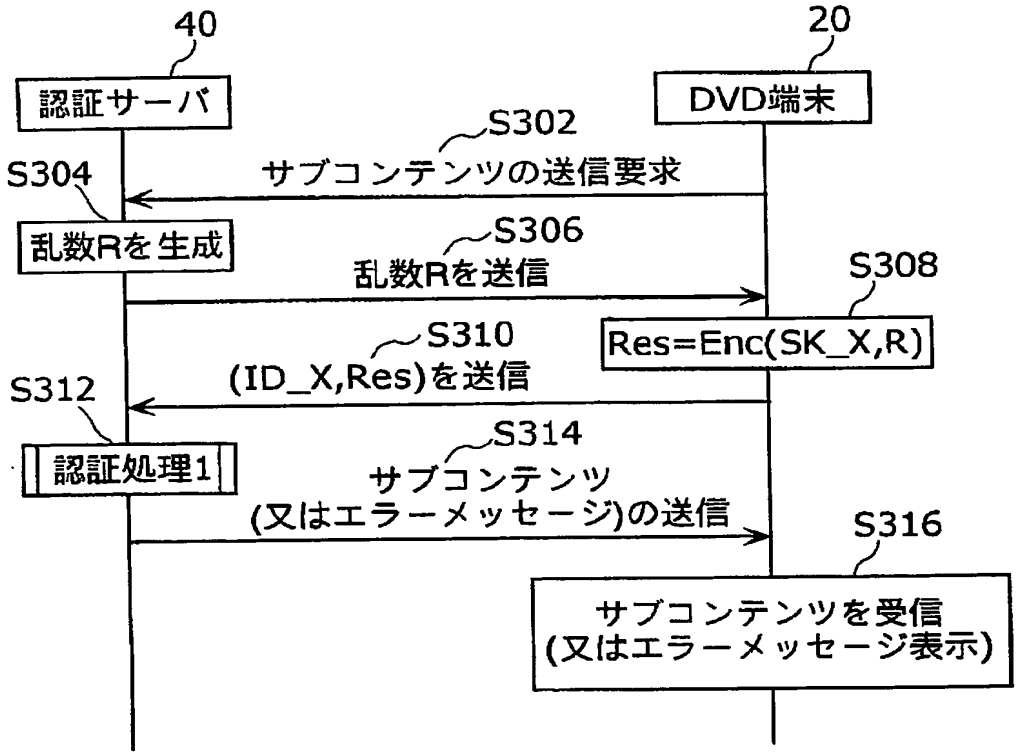
(a)

形式＋連番	端末ID	端末鍵	サブコンテンツのダウンロード履歴
DVM-1234-NNNNN	ABC5566	DEF7890	○○○ディレクターズカット版 ・・・
DVM-2345-NNNNN	UVW6677	XYZ8901	△△△メイキングフィルム ・・・
・・・	・・・	・・・	・・・

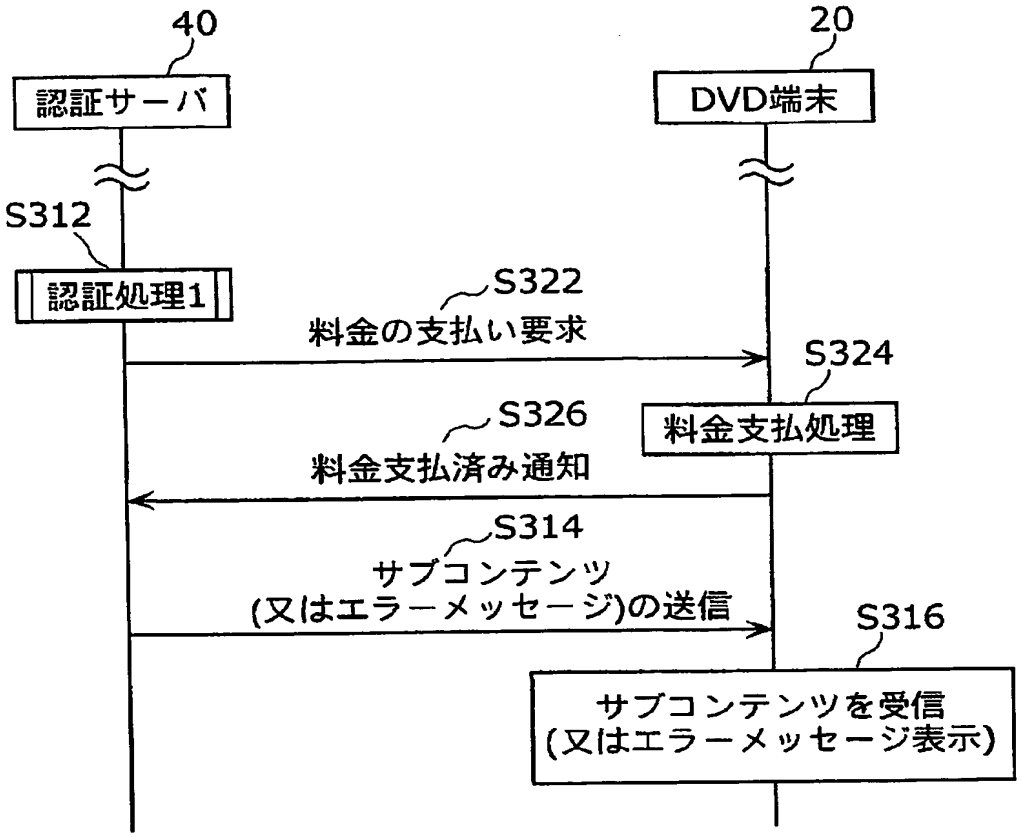
(b)

形式	端末鍵の総数	アクセス数
DVM-1234	10,000	18,500
DVM-5678	50,000	36,200
・・・	・・・	・・・

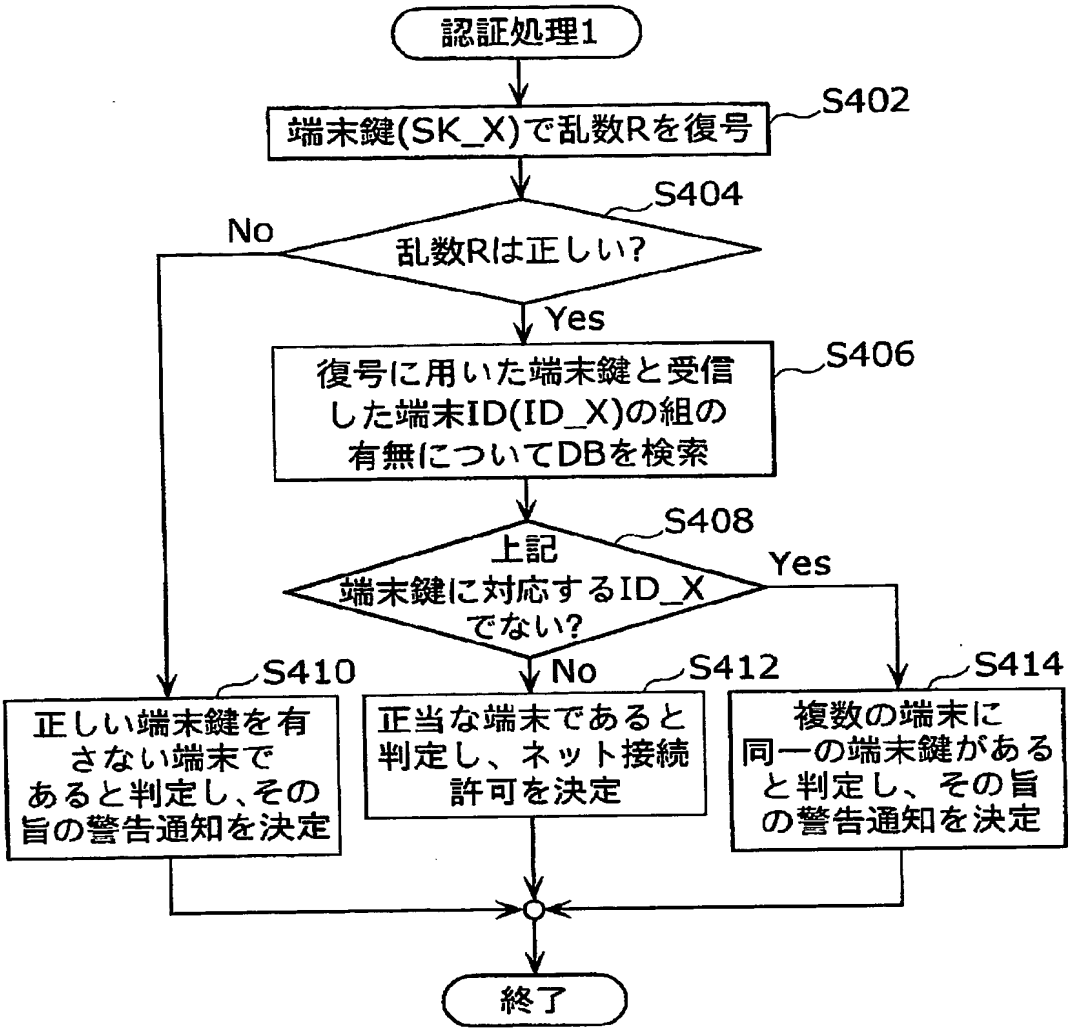
【図４】


40
認証サーバ
20
DVD端末
S302
サブコンテンツの送信要求
S304
乱数Rを生成
S306
乱数Rを送信
S308
Res=Enc(SK_X,R)
S310
(ID_X,Res)を送信
S312
認証処理1
S314
サブコンテンツ
(又はエラーメッセージ)の送信
S316
サブコンテンツを受信
(又はエラーメッセージ表示)

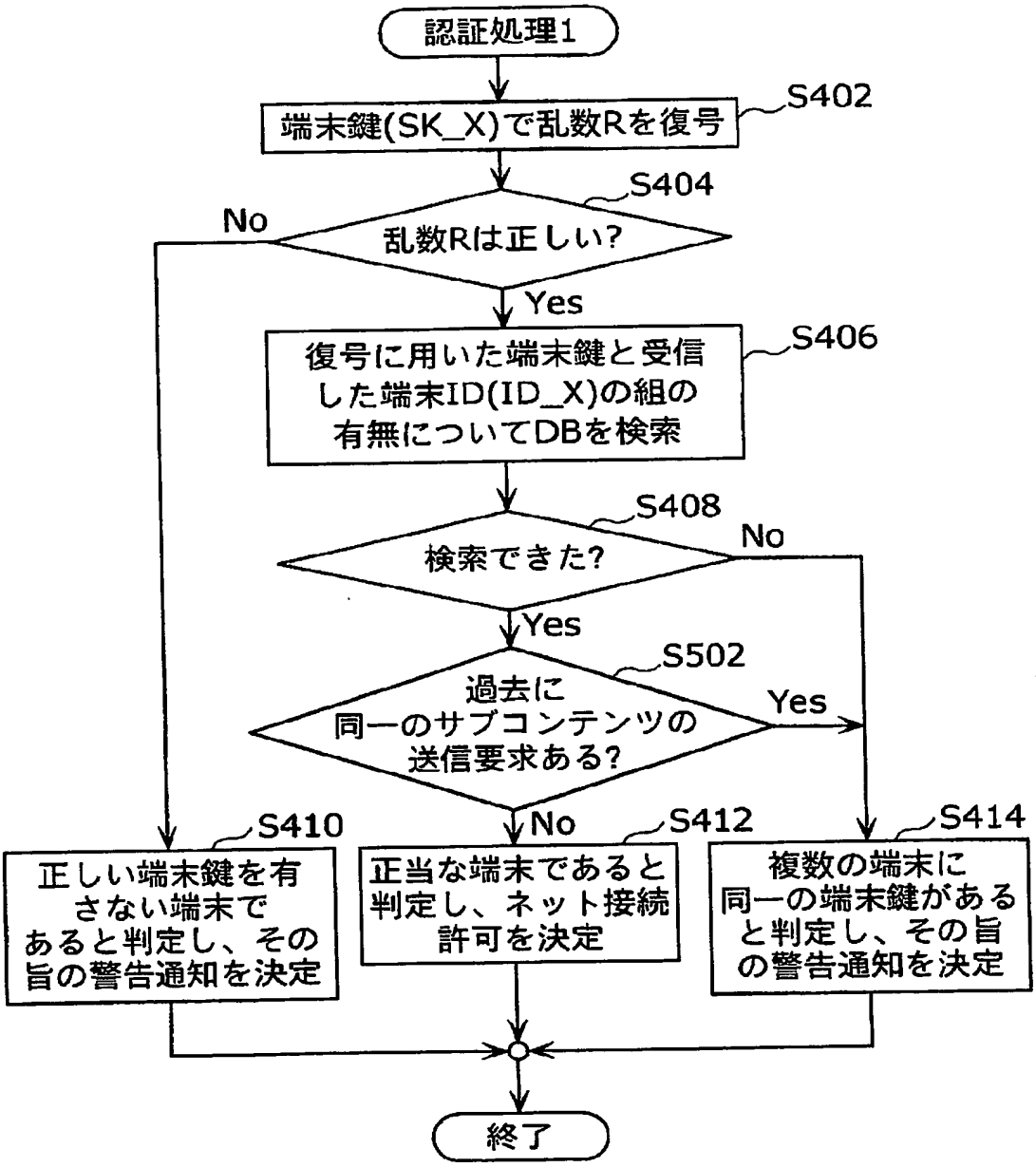
【図５】


40
認証サーバ
20
DVD端末
S312
認証処理1
S322
料金の支払い要求
S324
料金支払処理
S326
料金支払済み通知
S314
サブコンテンツ
(又はエラーメッセージ)の送信
S316
サブコンテンツを受信
(又はエラーメッセージ表示)

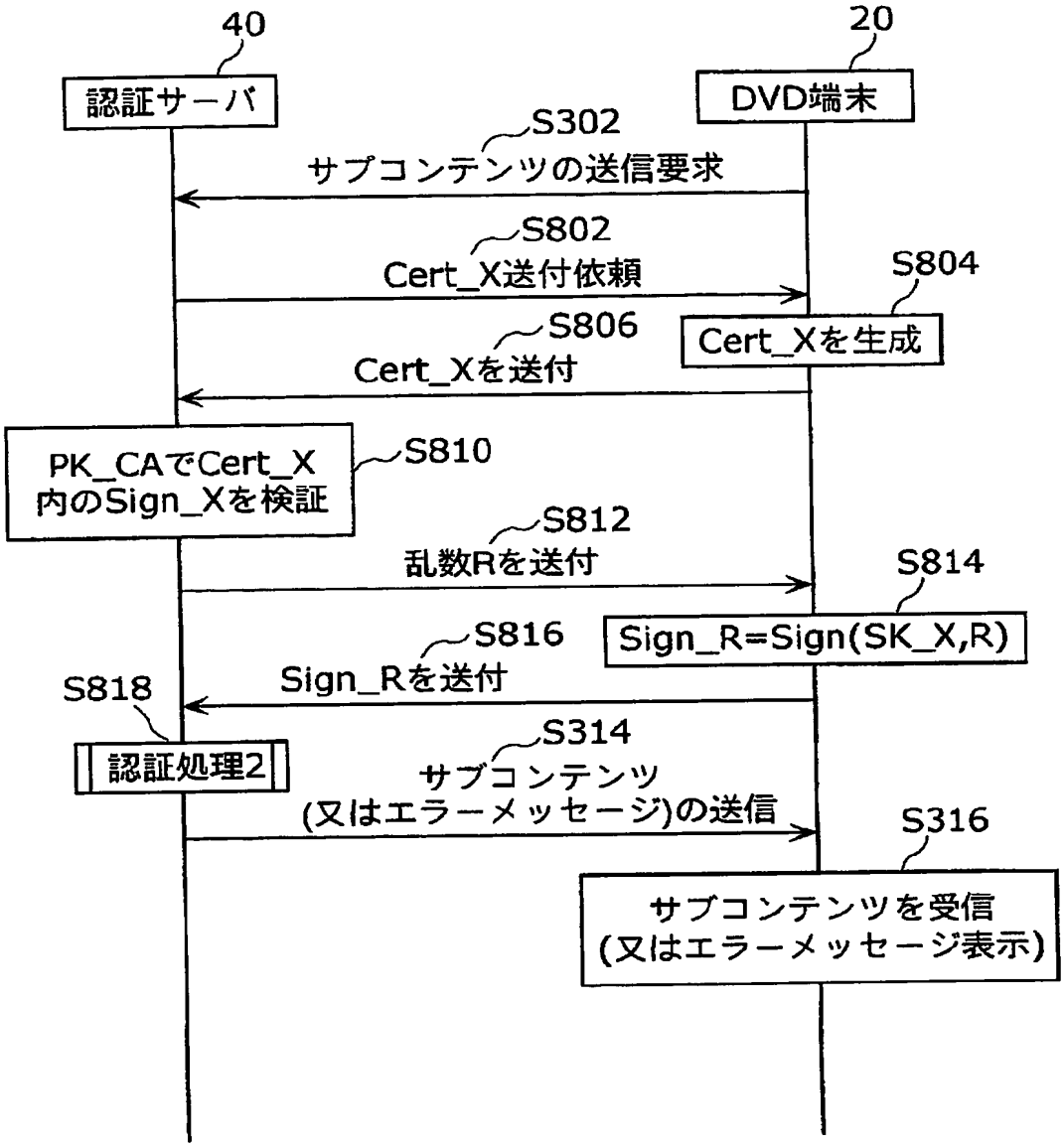
【図６】


認証処理1
端末鍵(SK_X)で乱数Rを復号
S402
S404
乱数Rは正しい?
No
Yes
復号に用いた端末鍵と受信した端末ID(ID_X)の組の有無についてDBを検索
S406
S408
上記端末鍵に対応するID_Xでない?
Yes
No
S410
正しい端末鍵を有さない端末であると判定し、その旨の警告通知を決定
S412
正当な端末であると判定し、ネット接続許可を決定
S414
複数の端末に同一の端末鍵があると判定し、その旨の警告通知を決定
終了

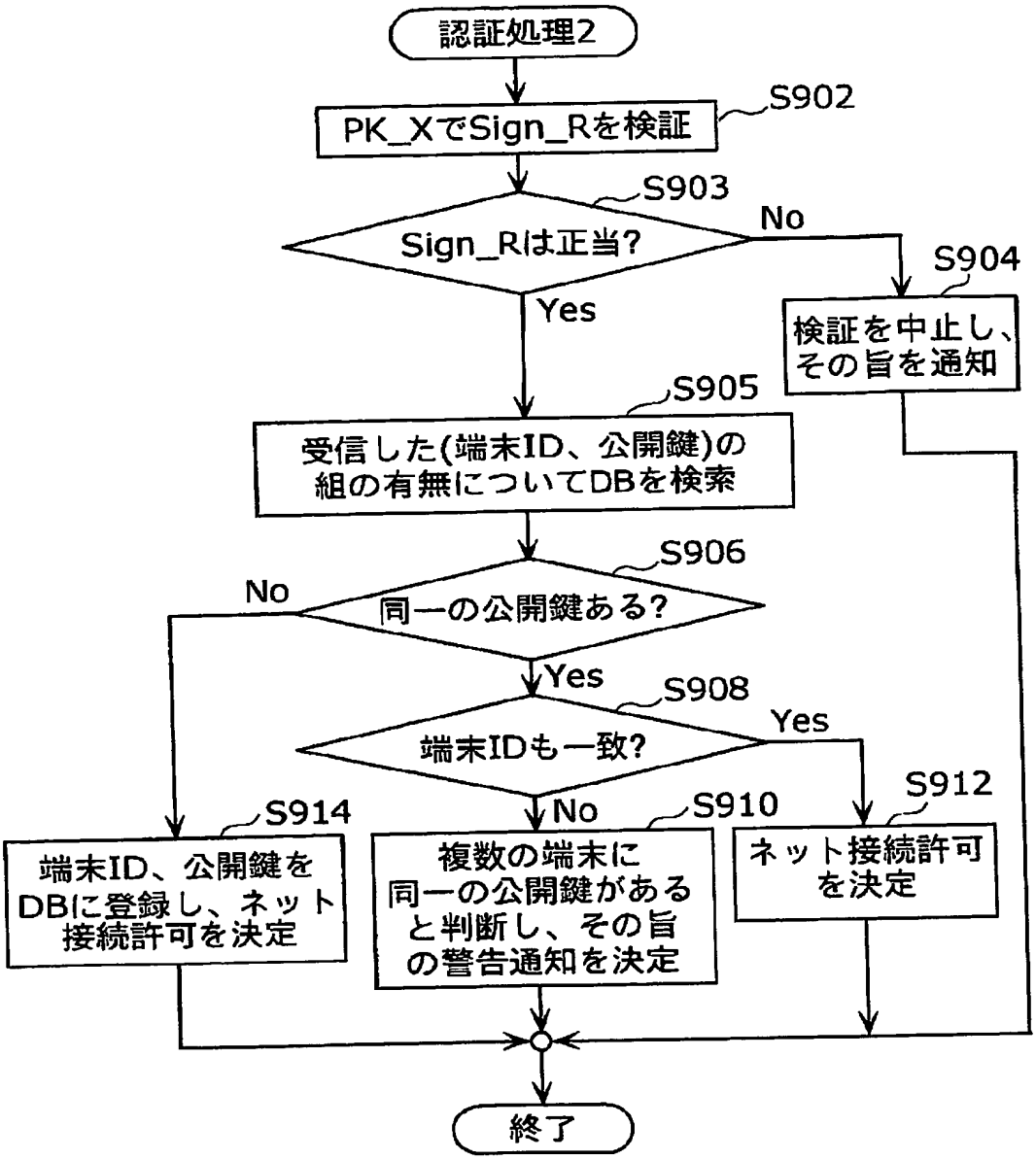
【図７】


認証処理1
端末鍵(SK_X)で乱数Rを復号
S402
S404
乱数Rは正しい?
No
Yes
復号に用いた端末鍵と受信した端末ID(ID_X)の組の有無についてDBを検索
S406
S408
検索できた?
No
Yes
S502
過去に同一のサブコンテンツの送信要求ある?
Yes
No
S410
正しい端末鍵を有さない端末であると判定し、その旨の警告通知を決定
S412
正当な端末であると判定し、ネット接続許可を決定
S414
複数の端末に同一の端末鍵があると判定し、その旨の警告通知を決定
終了

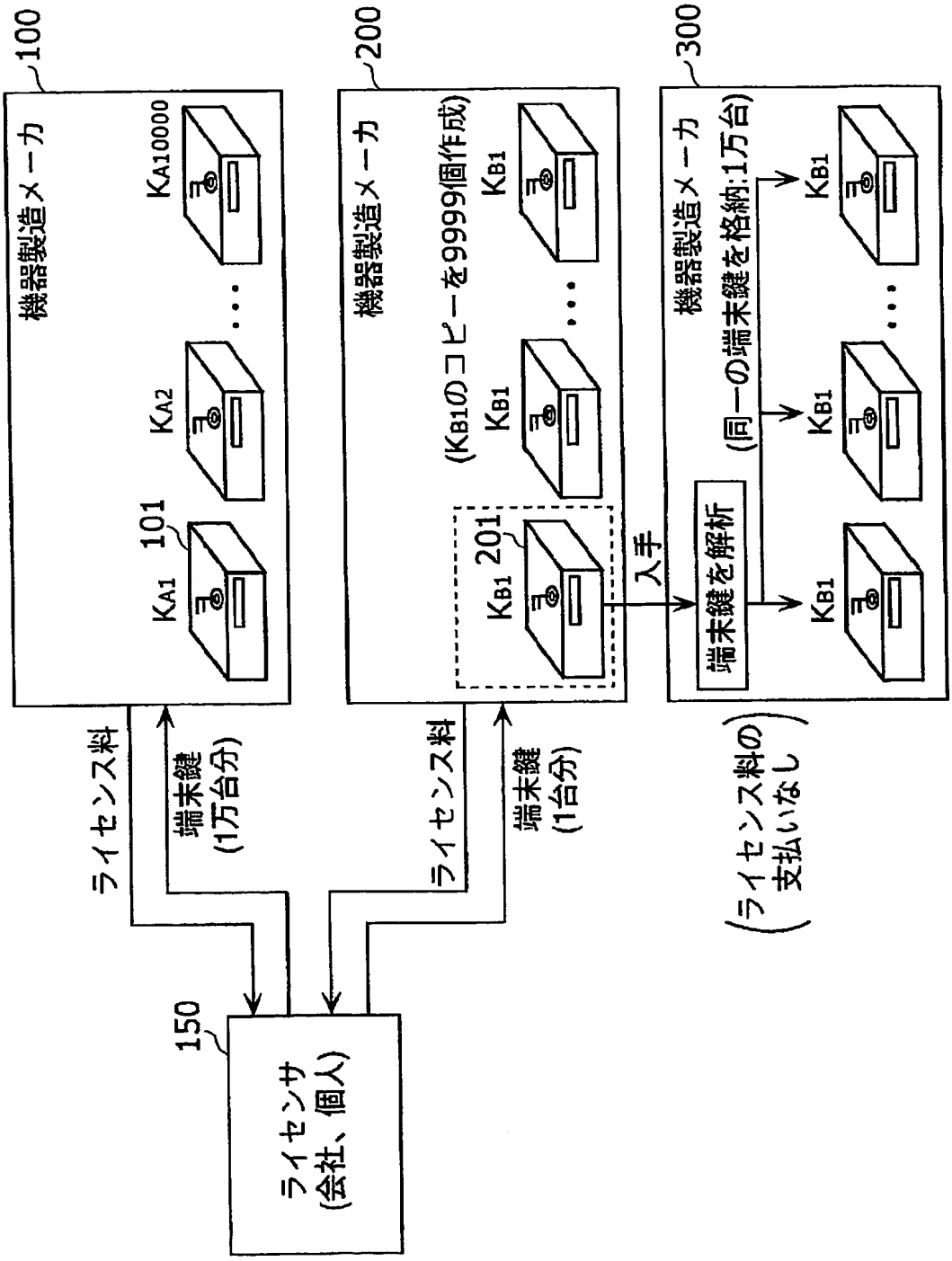
【図８】


40
認証サーバ
20
DVD端末
S302
サブコンテンツの送信要求
S802
Cert_X送付依頼
S804
Cert_Xを生成
S806
Cert_Xを送付
PK_CAでCert_X
内のSign_Xを検証
S810
S812
乱数Rを送付
S814
Sign_R=Sign(SK_X,R)
S816
Sign_Rを送付
S818
認証処理2
S314
サブコンテンツ
(又はエラーメッセージ)の送信
S316
サブコンテンツを受信
(又はエラーメッセージ表示)

【図９】


認証処理2
PK_XでSign_Rを検証
S902
S903
Sign_Rは正当?
No
S904
検証を中止し、その旨を通知
Yes
S905
受信した(端末ID、公開鍵)の組の有無についてDBを検索
S906
No
同一の公開鍵ある?
Yes
S908
端末IDも一致?
Yes
S912
ネット接続許可を決定
No
S910
複数の端末に同一の公開鍵があると判断し、その旨の警告通知を決定
S914
端末ID、公開鍵をDBに登録し、ネット接続許可を決定
終了

【図１０】


100
機器製造メーカ
KA10000
KA2
KA1
101
200
機器製造メーカ
(KB1のコピーを9999個作成)
KB1
KB1
KB1
201
300
機器製造メーカ
端末鍵を解析
(同一の端末鍵を格納:1万台)
KB1
KB1
KB1
入手
ライセンス料
端末鍵
(1万台分)
ライセンス料
端末鍵
(1台分)
(ライセンス料の
支払いなし)
150
ライセンサ
(会社、個人)

【書類名】要約書
【要約】
【課題】　複数の端末に同一の端末鍵が格納されていることや不正端末にどの正当な端末の端末鍵が格納されているかを検出し得る認証用サーバ装置、不正端末検出方法などを提供する。
【解決手段】　ＤＶＤ端末２０は、認証サーバ４０にサブコンテンツの送信要求を行う（Ｓ３０２）。認証サーバ４０は、乱数Ｒを生成し（Ｓ３０４）、ＤＶＤ端末２０に送信する（Ｓ３０６）。ＤＶＤ端末２０は、端末情報記憶部２５に記憶している端末鍵と端末ＩＤを読み出し、端末鍵（ＳＫ＿Ｘ）で、受信した乱数Ｒを暗号化し（Ｓ３０８）、これと端末ＩＤ（ＩＤ＿Ｘ）とを認証サーバ４０に送信する（Ｓ３１０）。認証サーバ４０は、ＤＶＤ端末２０から受信した暗号化された乱数Ｒ及び端末ＩＤについて検証し、ＤＶＤ端末２０が正当な端末か否かを認証する（Ｓ３１２）。
【選択図】　図４

認定・付加情報

特許出願の番号	特願２００４－００９８６１
受付番号	５０４０００７３７５５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　１月１９日

＜認定情報・付加情報＞

【提出日】　平成16年 1月16日

特願２００４－００９８６１

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019488

International filing date: 20 December 2004 (20.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-009861
Filing date: 16 January 2004 (16.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse